

Reduced-Complexity Collaborative Decoding of Interleaved Reed-Solomon and Gabidulin Codes

Hans Kurzweil*, Mathis Seidl† and Johannes B. Huber†

*Department Mathematik, Universität Erlangen-Nürnberg, Erlangen, Germany

†Lehrstuhl für Informationsübertragung, Universität Erlangen-Nürnberg, Erlangen, Germany

Email: kurzweil@mi.uni-erlangen.de, {seidl, huber}@lnt.de

Abstract—An alternative method for collaborative decoding of interleaved Reed-Solomon codes as well as Gabidulin codes for the case of high interleaving degree is proposed. As an example of application, simulation results are presented for a concatenated coding scheme using polar codes as inner codes.

I. INTRODUCTION

Reed-Solomon (RS) codes are used in many applications, often implemented in an interleaved form as outer codes in concatenated code designs. By combining and interleaving a number $l \in \mathbb{N}$ of RS codewords, correction of long error bursts affecting only a few symbols of the particular underlying codewords can be achieved.

The standard decoding procedure consists of decoding each of the interleaved codewords separately. In recent years, methods have been investigated which try to decode the individual codewords no longer independently but in one step, allowing for error correction beyond half the minimum distance d . However, in order to decode the maximum possible number of errors $f = (d-2)$, the error vectors are required to be linearly independent.

In [1] and [2], a collaborative decoding algorithm for general linear codes based on Gaussian elimination is derived which is able to correct errors up to $\min\{l, d-2\}$ by solving a reduced system of l linear equations. Therefore, it is applicable only for situations where l can be chosen sufficiently high. Other methods based on multisequence shift-register synthesis (MSSRS) [3], [4] consider the complete system of key equations leading to an increased error correcting radius beyond l (but likewise smaller than $d-1$) and an improved decoding performance. While the decoding complexity is of same order $\mathcal{O}(lf^2)$ for both approaches, in case of high interleaving degrees the first method might be preferable from a computational point of view as the Gaussian elimination allows for parallelized computing of rows and columns (and thus for a reduced decoding delay) in contrast to the sequential structure of the shift register synthesis algorithm.

Our considerations are based on the method from [1] and [2]. We adopt the results for the special case of RS codes. In contrast to [1], by using a specific code we obtain a unique solution in terms of an error locator polynomial rather than a superset of the error locations. More importantly, only the first part of each syndrome sequence is required for decoding. Furthermore, we will show that in the case of concatenated

codes with high interleaving degree ($l \geq d-2$), the performance degradation compared to MSSRS is small.

II. REED-SOLOMON CODES AND INTERLEAVING

The authors are aware that the theory of RS codes is widely known. However, since our considerations are based on extended, non-standard RS codes, a short introduction seems to be necessary as well. Although even more general definitions as in [5] would be possible, we define a Generalized Reed-Solomon (GRS) code of length n and dimension k over a finite field \mathbb{F} with $|\mathbb{F}| = q$ elements as follows:

Definition 1 (Reed-Solomon code). Let $\mathbf{v} := (v_1, \dots, v_n) \in \mathbb{F}^n$ be a row vector of $n \leq q$ different elements of \mathbb{F} . Let further \mathcal{P}_k ($k < n$) be the vector space of polynomials over \mathbb{F} with degree $< k$. Then a Reed-Solomon code $\mathcal{GRS}(q; n, k, \mathbf{v})$ is defined as the set of evaluations at \mathbf{v}

$$\left\{ (p(v_1), p(v_2), \dots, p(v_n)) \in \mathbb{F}^n : p \in \mathcal{P}_k \right\}$$

of all the polynomials from \mathcal{P}_k .

Definition 2. A Reed-Solomon-Code $\mathcal{GRS}(q; n, k, \mathbf{v})$ with length $n = q-1$ and

$$\mathbf{v} = (\alpha^0, \alpha^1, \dots, \alpha^{q-2})$$

with α being a primitive element of \mathbb{F} will be referred to as $\mathcal{RS}(q-1, k)$.

The extended code of length $n = q$ obtained by adding the zero element of \mathbb{F} to the vector \mathbf{v} of $\mathcal{RS}(q-1, k)$, i.e.

$$\mathbf{v} = (0, \alpha^0, \alpha^1, \dots, \alpha^{q-2}),$$

will be called $\mathcal{RS}^*(q, k)$.

The code $\mathcal{RS}^*(q, k)$ has one interesting property which has been proved in a more general form in [5, p. 304] and will be the foundation of our following considerations:

Lemma 1. The dual code of $\mathcal{RS}^*(q, k)$ is $\mathcal{RS}^*(q, q-k)$, i.e. the Vandermonde matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \\ 0 & 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \alpha^{m-1} & \alpha^{2(m-1)} & \dots & \alpha^{(q-2)(m-1)} \end{pmatrix}$$

with $m := n-k$ is a possible parity check matrix of $\mathcal{RS}^*(q, k)$.

According to Lemma 1, syndrome calculations in the case of \mathcal{RS}^* codes are actually polynomial evaluations. Moreover, we will show in the following that linear combinations of the rows of \mathbf{H} lead directly to coefficients of polynomials, the roots of which will specify the error locations.

By grouping $l \in \mathbb{N}$ codewords of $\mathcal{GRS}(q; n, k, \mathbf{v})$ column-wise to a $(n \times l)$ -matrix, we obtain a linear code of length $(l \cdot n)$, dimension $(l \cdot k)$ and minimum distance $(n - k + 1)$ like the individual codes.

Definition 3 (Interleaved Reed-Solomon (IRS) code). *Given a certain Reed-Solomon code $\mathcal{C} := \mathcal{GRS}(q; n, k, \mathbf{v})$, we define an Interleaved Reed-Solomon code $\mathcal{IRS}(q; l, n, k, \mathbf{v})$ of interleaving degree l as the set of $(n \times l)$ -matrices*

$$\left\{ \mathbf{A} = \left(\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \dots, \mathbf{a}^{(l)} \right) : (\mathbf{a}^{(i)})^\top \in \mathcal{C}, i = 1, \dots, l \right\},$$

each consisting of l column-wise arranged codewords from \mathcal{C} . In case of $\mathcal{C} = \mathcal{RS}^(q, k)$, the resulting IRS code will be referred to as $\mathcal{IRS}^*(q, l, k)$.*

III. COLLABORATIVE DECODING

Assume now that a codeword $\mathbf{A} \in \mathcal{IRS}^*(q, l, k)$ is transmitted over an additive noise channel, so that

$$\mathbf{Y} = \mathbf{A} + \mathbf{E} \in \mathbb{F}^{n \times l}$$

with some error matrix $\mathbf{E} \in \mathbb{F}^{n \times l}$ is received at the channel output. Let \mathbf{E} be a matrix with exactly $f \in \mathbb{N}$ non-zero rows. We denote \mathcal{F} the set of indices of these erroneous rows. (Clearly, at first f and \mathcal{F} are unknown to the decoder.)

For collaborative decoding, we arrange the l syndrome sequences generated from \mathbf{Y} as columns of a so-called syndrome matrix \mathbf{S} . The computation can be written formally as a matrix multiplication of \mathbf{Y} with the parity check matrix \mathbf{H} of the underlying \mathcal{RS}^* code:

$$\mathbf{S} = \mathbf{H} \cdot \mathbf{Y} = \mathbf{H} \cdot (\mathbf{A} + \mathbf{E}) = \mathbf{H} \cdot \mathbf{E} = \mathbf{H}^\mathcal{F} \cdot \mathbf{E}_\mathcal{F} \quad (1)$$

with $\mathbf{H}^\mathcal{F}$ and $\mathbf{E}_\mathcal{F}$ denoting the submatrices of \mathbf{H} and \mathbf{E} consisting only of those columns and rows, respectively, whose indices are contained in \mathcal{F} . The last equivalence holds because all other rows of \mathbf{E} are zero. The syndrome matrix takes the form

$$\mathbf{S} = \begin{pmatrix} s_1^{(1)} & \dots & s_1^{(l)} \\ \vdots & \ddots & \vdots \\ s_{n-k}^{(1)} & \dots & s_{n-k}^{(l)} \end{pmatrix} \in \mathbb{F}^{(n-k) \times l}. \quad (2)$$

Instead of successively solving (for increasing f^*) the complete system of $l \cdot (n - k - f)$ key equations

$$s_i^{(m)} = \sum_{j=1}^{f^*} \lambda_j s_{i-j}^{(m)}, \quad i = f^* + 1, \dots, n - k \quad (3)$$

$$m = 1, \dots, l$$

for the coefficients $\lambda_j \in \mathbb{F}$ of the error locator polynomial ($\lambda_0 := 1$), we use a subsystem consisting of l equations only to be solved:

$$s_{f^*+1}^{(m)} = \sum_{j=1}^{f^*} \lambda_j s_{f^*+1-j}^{(m)}, \quad m = 1, \dots, l \quad (4)$$

From (4) it follows immediately that the error correcting radius, i.e. the maximum number of erroneous rows that can be corrected, cannot be greater in our case than

$$f_{\max} := \min\{l, d - 2\} \quad (5)$$

The decoding task then plainly consists in determination of the row of \mathbf{S} with smallest index ($f^* + 1$) that can be written as a linear combination of the former rows. By applying the Gauss-Jordan algorithm to the columns of \mathbf{S} , we obtain the reduced column echelon form (rcef) of \mathbf{S} :

$$\text{rcef}(\mathbf{S}) = \begin{pmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & 0 \\ 0 & \dots & 1 & 0 & \dots & 0 \\ \lambda_1 & \dots & \lambda_{f^*} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}. \quad (6)$$

Our decoding algorithm will be successful whenever the following two conditions are fulfilled:

Cond. 1 : The non-zero rows \mathbf{E}_i ($i \in \mathcal{F}$) of the error matrix are linearly independent.

Cond. 2 : $f \leq f_{\max}$ holds.

Actually, **Cond. 1** and **Cond. 2** are both necessary and sufficient for correct decoding. We will make some remarks on the linear independence condition **Cond. 1** later in section V.

Theorem 1. *If **Cond. 1** and **Cond. 2** are fulfilled, then $f^* = f$ and the polynomial*

$$\Lambda(x) = x^{f^*} - \sum_{j=1}^{f^*} \lambda_j x^{j-1}$$

built from the elements λ_j from (6) is the error locator polynomial, i.e.

$$\Lambda(v_i) = 0 \quad \Leftrightarrow \quad i \in \mathcal{F}$$

holds.

Proof: See the Appendix. ■

Obviously, only the first $(f + 1)$ rows of \mathbf{S} rather than the complete (length $n - k$) syndrome sequences are necessary for finding Λ . Thus, especially if the actual number of errors is small, the computational complexity can be reduced significantly by successive calculation of the rows of \mathbf{S} . We will discuss this version in section VI.

IV. CODEWORD RECONSTRUCTION

Given the (correctly computed) set \mathcal{F} of erroneous columns of \mathbf{Y} , we are now able to reconstruct $\mathbf{E}_\mathcal{F}$ and therefore $\mathbf{A} = \mathbf{Y} - \mathbf{E}$. The matrix equation

$$\mathbf{S} = \mathbf{H}^\mathcal{F} \cdot \mathbf{E}_\mathcal{F} \quad (7)$$

defines an over-determined system of linear equations consisting of $l \cdot (n - k)$ equations and $l \cdot f$ unknowns. Since we know that (7) must have a unique solution and since the first f rows of the (Vandermonde!) matrix $\mathbf{H}^\mathcal{F}$ are linearly independent, we can restrict to the smaller system

$$\mathbf{S}_{[f]} = \mathbf{H}_{[f]}^\mathcal{F} \cdot \mathbf{E}_\mathcal{F} \quad (8)$$

with $\mathbf{S}_{[f]}$ and $\mathbf{H}_{[f]}^{\mathcal{F}}$ denoting the matrices consisting of the first f rows of \mathbf{S} and $\mathbf{H}^{\mathcal{F}}$, respectively. As mentioned before, $\mathbf{H}_{[f]}^{\mathcal{F}}$ is a quadratic - and thus invertible - Vandermonde matrix and (8) actually an interpolation problem.

Note that also for calculation of the error values the last rows $\mathbf{S}_{f+2}, \dots, \mathbf{S}_{n-k}$ of the syndrome matrix \mathbf{S} are not required.

V. FAILURE PROBABILITY

As shown before, in case of $f \leq f_{\max}$ the success of the decoding procedure solely depends on the linear independence of the error vectors. If we assume that the \mathbf{E}_i are random vectors uniformly distributed over $\mathbb{F}^l \setminus \{\mathbf{0}\}$, the probability that *Cond. 1* is not fulfilled, i.e. that the \mathbf{E}_i are linearly dependent, can be overbounded for $f \geq 2$ by

$$q^{-(l+1-f)} \cdot \frac{1 - q^{-f}}{1 - q^{-1}} \approx q^{-(l+1-f)}, \quad (9)$$

as shown in [1]. Clearly, the decoder certainly fails if the number of erroneous columns exceeds f_{\max} . Thus,

$$P_f(f, l) \leq \begin{cases} 0 & f < 2 \\ q^{-(l+1-f)} & 2 \leq f \leq f_{\max} \\ 1 & \text{else} \end{cases} \quad (10)$$

holds as an upper bound for the failure probability under assumption of uniformly distributed error vectors.

Compared to the failure probabilities of the Feng-Tzeng algorithm as derived in [4], the probabilities for the decoding to fail are equivalent for $f = f_{\max} = (n - k - 1)$, but decline significantly slower as f decreases. Moreover, for $l < (n - k - 1)$ the error correction radius of the Feng-Tzeng algorithm, i.e. the number of correctable errors, is in general strictly greater than in our case.

In concatenated code designs where the columns of an outer IRS code are encoded by an inner block code, the overall frame error rate (FER) can be analytically determined by

$$\text{FER} = \sum_{t=2}^N \binom{N}{t} \cdot P_f(t, l) \cdot p^t \cdot (1 - p)^{N-t}. \quad (11)$$

with p being the frame error rate of the inner code.

Fig. 1 depicts the bounds on the FER as a function of the inner code error rate p for various interleaving degrees in the range from 9 to 15. Here, a (204, 188) shortened RS code like in the DVB standard [6] is used. For comparison, the failure bounds for MSSRS are plotted as dashed grey lines.

Whereas for small interleaving degrees l the multisequence decoder (the lines of which coincide for $l = 9 \dots 14$!) clearly outperforms our method, for $l \geq 14$ the performance of both approaches is nearly identical.

VI. COMPLEXITY

The computational complexity of the Gauss-Jordan algorithm is of same order $\mathcal{O}(lf^2)$ like the independent decoder as well as the multisequence synthesis algorithm (with l and f as defined before).

As already mentioned, only the first $(f + 1)$ rows rather than the whole matrix \mathbf{S} are actually necessary for determination

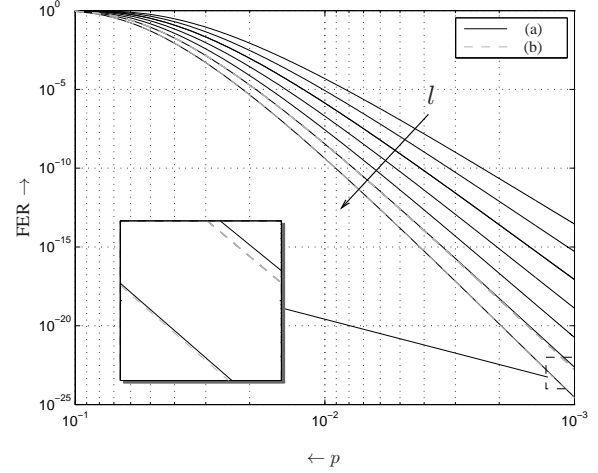


Fig. 1. Bounds on the frame error rate (FER) for a (204, 188) IRS code with $l = 9 \dots 15$ for collaborative decoding using (a) Gaussian elimination and (b) multisequence shift-register synthesis (MSSRS)

of the error locator polynomial. In particular, when $f \ll l$ the computational complexity may be significantly reduced by combining syndrome calculation and actual decoding, i.e. by applying a decoding algorithm which in each step $t = 1 \dots f + 1$ calculates one additional row of \mathbf{S} and performs Gaussian elimination on the corresponding $(t \times l)$ -submatrix of \mathbf{S} until a linearly dependent row is detected. Therefore, the complexity of the syndrome calculations reduces to $\mathcal{O}(lnf)$ rather than $\mathcal{O}(lnd)$. In the extreme case that no errors have occurred, the decoder stops without performing even a single finite field multiplication since, due to the special form of \mathbf{H} , the first coefficient of the l syndrome sequences each simply consists of a column sum of \mathbf{Y} .

Moreover, in each step of the Gaussian elimination, the l columns of the syndrome matrix \mathbf{S} may be transformed at the same time by a parallel implementation of the decoder in order to achieve further reductions in decoding delay.

VII. A NOTE ON GABIDULIN CODES

Gabidulin codes [7] are a class of linear rank metric codes which play an important role in random linear network coding [8]. Their codewords can be represented either as $(m \times n)$ -matrices over a finite field with q elements \mathbb{F}_q or equivalently as vectors over the extension field \mathbb{F}_{q^m} .

For decoding l -interleaved Gabidulin codes, a key equation for computing the error span polynomial from the syndromes can be derived (cf. [9]) analogously to the case of IRS codes (4):

$$\mathbf{S}_{f+1} = \sum_{j=1}^f \lambda_j (\mathbf{S}_{f+1-j})^{[j]} \in \mathbb{F}_{q^m}^l, \quad (12)$$

where the operator $[j]$ denotes the pointwise applied q^j -th power of a vector.

With a slight modification, i.e. by raising the current row \mathbf{S}_j of \mathbf{S} to the power $[j]$ in each elimination step, the algorithm presented in this paper is applicable to decoding of interleaved

Gabidulin codes as well. In this case, an analogue to the failure bound for IRS codes (10) is obtained for decoding interleaved Gabidulin codes:

Theorem 2. *The failure probability in case of uniformly distributed rank- f error words is upper bounded by*

$$P_f^G(f, l) \leq \begin{cases} 0 & f < 2 \\ 4 \cdot (q^m)^{-(l+1-f)} & 2 \leq f \leq \min\{l, d-2\} \\ 1 & \text{else} \end{cases} \quad (13)$$

where d denotes the minimum rank distance of the underlying Gabidulin code.

Proof: A proof similar to the proof of Theorem 3.11 in [10] is given in the Appendix. ■

VIII. CODE CONCATENATION

The derivations of failure bounds on the FER here as well as in [4] remain valid only as long as the error vectors are distributed uniformly over $\mathbb{F}^l \setminus \{0\}$. In [4], it was demonstrated for small interleaving degrees ($l = 3$) that the performance degradation due to a different error distribution can be neglected when using tailbiting convolutional codes as inner codes. Unfortunately, in case of large inner code lengths (> 100) this result does not hold anymore as convolutional codes produce error vectors of relatively small weight. Instead of applying randomizing methods which do not only permute the error bits but also increase their amount while introducing additional computational complexity, we propose the use of an alternative inner coding.

Polar codes [11], first introduced by E. Arkan, are decoded by a low-complexity successive decoder which generates estimations on the source bits one after another, each depending on the decisions made before. In case of a wrong decision, long error sequences up to the end of the codeword are produced. This fact (which could usually be seen as a drawback) makes polar codes well suited as inner codes in our case. However, the polar successive decoder happens to fail at certain bits significantly more likely than at other ones. Therefore, in order to meet *Cond. 1* it appears favorable to apply random permutations to the information bits of the polar code, different for each row of the IRS codeword.

IX. SIMULATION RESULTS

Finally, we present some exemplary simulations to demonstrate the tightness of the derived bounds and to show that the assumption of random error vectors can be realized in practice. As an application example closely related to the DVB-X standards (first version) [6], a (256,128) polar code as inner code together with the (204,188) IRS code from section V is used. As the corresponding IRS code is able to correct up to 15 erroneous columns, we chose an interleaving degree of $l = 16$ rather than $l = 12$ in the DVB standard. In Fig. 2, the frame error rate (FER-) performance of the concatenation design including polar codes is compared to a concatenation of an inner rate 1/2 convolutional code (constraint length $K = 7$)

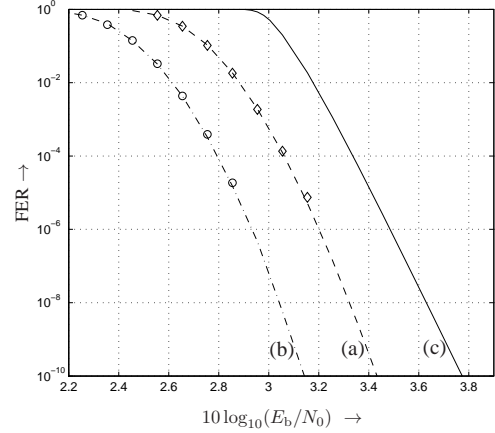


Fig. 2. Simulated and analytical frame error rate (FER-) performance of a $l = 16$ concatenated code with an outer RS(204,188) code and (a) an inner (256,128) polar code with standard decoding, (b) an inner (256,128) polar code with improved decoding, (c) an inner rate 1/2 convolutional code with constraint length $K = 7$

with an independently decoded outer (204,188) RS code as used in the DVB standard. By using an improved polar decoding scheme as considered in [12], the performance can be further enhanced by about 0.3 dB. Simulation results of those improved polar codes are represented by circular markers. Fig. 2 shows that the simulation points of both decoding schemes meet the theoretical failure bound very accurately. Both IRS-polar concatenation schemes clearly outperform the DVB code in terms of frame error rates as well as of computational complexity.

APPENDIX

A. Proof of Theorem 1:

Let $f < (n-k)$ denote the actual number of erroneous rows and \mathcal{F} the set of their indices (both being at first unknown to the decoder). The square submatrix of \mathbf{H}

$$\mathbf{K} := (\mathbf{H}^{\mathcal{F}})_{[f]} \in \mathbb{F}^{f \times f}, \quad (14)$$

consisting of the first f rows and the columns with indices from \mathcal{F} of \mathbf{H} , is a Vandermonde and thus non-singular matrix of full rank f . Therefore, the $(f+1)$ th row of $\mathbf{H}^{\mathcal{F}}$

$$\boldsymbol{\mu} := (\mathbf{H}^{\mathcal{F}})_{f+1} \in \mathbb{F}^f \quad (15)$$

is a unique linear combination of the first f rows \mathbf{K}_j of \mathbf{K} :

$$\boldsymbol{\mu} = \sum_{j=1}^f \lambda_j \mathbf{K}_j \quad (16)$$

for some $\lambda_j \in \mathbb{F}$, $j = 1, \dots, f$. We will now demonstrate how these coefficients λ_j can be derived from the syndrome matrix \mathbf{S} . Let φ be the linear mapping defined by $\mathbf{E}_{\mathcal{F}} \in \mathbb{F}^{f \times l}$:

$$\varphi : \mathbb{F}^f \mapsto \mathbb{F}^l, \quad \mathbf{v} \mapsto \mathbf{v} \cdot \mathbf{E}_{\mathcal{F}}. \quad (17)$$

By definition of \mathbf{K} and $\boldsymbol{\mu}$,

$$\begin{aligned} \varphi(\mathbf{K}_j) &= \mathbf{S}_j, \quad j = 1, \dots, f \\ \varphi(\boldsymbol{\mu}) &= \mathbf{S}_{f+1} \end{aligned}$$

By our assumption *Cond. 1*, $\mathbf{E}_{\mathcal{F}}$ is a matrix of rank f . Thus, φ is an injective mapping, and the vectors \mathbf{S}_j ($j = 1, \dots, f$) form a basis of the image $\varphi(\mathbb{F}^f) \subset \mathbb{F}^l$ of φ .

Consequently, the $(f+1)$ th row of \mathbf{S} is a linear combination of the former, uniquely determined by the very same coefficients λ_j as in (16):

$$\mathbf{S}_{f+1} = \varphi(\boldsymbol{\mu}) = \sum_{j=1}^f \lambda_j \varphi(\mathbf{K}_j) = \sum_{j=1}^f \lambda_j \mathbf{S}_j. \quad (18)$$

Thus, the actual number of errors f is given by the row of \mathbf{S} with minimum index that can be written as a linear combination of the preceding rows. It is clear that this index as well as the coefficients λ_j can be calculated by performing elementary column operations on \mathbf{S} .

Given these coefficients, we define a polynomial

$$\Lambda(x) := x^f - \sum_{j=1}^f \lambda_j x^{j-1}. \quad (19)$$

Due to the special form of \mathbf{H} (cf. Lemma 1), the i th column \mathbf{H}^i consists of the consecutive powers of $v_i \in \mathbb{F}$. Consequently,

$$0 = \Lambda(x_i) = x_i^f - \sum_{j=1}^f \lambda_j x_i^{j-1} \quad (20)$$

holds if and only if $i \in \mathcal{F}$. Since Λ is a polynomial of degree $f = |\mathcal{F}|$, these are obviously the only roots. Therefore, Λ is the error locator polynomial. ■

B. Proof of Theorem 2:

In the following, we will denote the rank of a $(n \times k)$ -matrix \mathbf{S} over an extension field \mathbb{F}_{q^m} of \mathbb{F}_q by $\text{rank}_{q^m}(\mathbf{S})$ while the rank of the corresponding $(n \times km)$ -matrix over \mathbb{F}_q will be referred to as $\text{rank}_q(\mathbf{S})$.

Let $\mathbf{E} \in \mathbb{F}_{q^m}^{n \times l}$ be an arbitrary additive error word of an l -interleaved Gabidulin code, chosen at random from the set of matrices with $\text{rank}_q(\mathbf{E}) = f < f_{\max}$. Let further $\mathbf{S} \in \mathbb{F}_{q^m}^{f \times l}$ denote the submatrix consisting of the first f rows of the corresponding syndrome matrix $\mathbf{H}\mathbf{E}$. As the parity check matrix \mathbf{H} is of maximum rank over \mathbb{F}_q , the possible matrices \mathbf{S} are uniformly distributed over the set

$$\mathcal{S}_f := \{\mathbf{A} \in \mathbb{F}_{q^m}^{f \times l} : \text{rank}_q(\mathbf{A}) = f\}.$$

It is known (cf. [13, p. 50]) that the mapping

$$\sigma_i : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m}, \quad \alpha \mapsto \alpha^{[i]} \quad (i \in \mathbb{N})$$

defines an automorphism of the field \mathbb{F}_{q^m} . Thus, there exists a one-to-one correspondence ψ between \mathcal{S}_f and the set of matrices defined by the key equation (12):

$$\psi : \mathbf{S} = (\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_f)^T \mapsto (\mathbf{S}_1, \mathbf{S}_2^{[1]}, \dots, \mathbf{S}_f^{[f-1]})^T$$

Obviously, the decoding will only fail if $\text{rank}_{q^m}(\psi(\mathbf{S})) < f$ for $\mathbf{S} \in \mathcal{S}_f$. In this case there exists a nontrivial linear combination $\mathbf{0} \neq \mathbf{v} \in \mathbb{F}_{q^m}^f$ such that

$$\mathbf{h} \cdot \psi(\mathbf{S}) = \mathbf{0} \in \mathbb{F}_{q^m}^l \quad (21)$$

holds. Because of $\text{rank}_{q^m}(\mathbf{h}) = 1$ there are at most

$$N_f := (q^m)^{l(f-1)}$$

possibilities to choose a matrix $\mathbf{S} \in \mathbb{F}_{q^m}^{f \times l}$ such that (21) is fulfilled. On the other hand, it is shown in [10] that

$$|\mathcal{S}_f| \geq \frac{1}{4} \cdot (q^m)^{lf}.$$

Consequently, for an arbitrary chosen \mathbf{v} , the probability that $\text{rank}_{q^m}(\psi(\mathbf{S})) < f$ for a randomly chosen matrix \mathbf{S} cannot be greater than

$$P_{\max} := \frac{N_f}{|\mathcal{S}_f|} \leq 4 \cdot (q^m)^{-l}.$$

Now the overall failure probability can be upper bounded by summing up over the number of all distinct null spaces defined by different choices of \mathbf{v} . This number is certainly smaller than

$$\frac{(q^m)^f - 1}{q^m - 1} \approx (q^m)^{f-1} =: N$$

because $\mathbf{v} \neq \mathbf{0}$ and because \mathbf{v} and $\alpha \mathbf{v}$ lead to the same null space for any nonzero $\alpha \in \mathbb{F}_{q^m}$.

Finally, $P_f^G(f, l)$ is bounded by

$$P_f^G(f, l) \leq P_{\max} \cdot N \leq 4 \cdot (q^m)^{-(l+1-f)}.$$

■

REFERENCES

- [1] J. Metzner and E. Kapturowski, "A general decoding technique applicable to replicated file disagreement location and concatenated code decoding," *IEEE Trans. Inf. Theor.*, vol. 36, no. 4, pp. 911–917, 1990.
- [2] C. Haslach and A.J. Han Vinck, "A decoding algorithm with restrictions to array codes," *IEEE Trans. Inf. Theor.*, vol. 45, no. 7, pp. 2339–2344, 1999.
- [3] Feng, G. L. and Tzeng, K. K., "A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Trans. Inf. Theor.*, vol. 37, no. 5, pp. 1274–1287, 1991.
- [4] G. Schmidt, V. Sidorenko and M. Bossert, "Collaborative decoding of interleaved Reed-Solomon codes and concatenated code designs," *IEEE Trans. Inf. Theor.*, vol. 55, no. 7, pp. 2991–3012, 2009.
- [5] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [6] ETSI EN 300 421 V1.1.2 (1997-08), "Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz satellite services."
- [7] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 1–12, 1985.
- [8] D. Silva, F. R. Kschischang and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theor.*, vol. 54, no. 9, pp. 3951–3967, 2008.
- [9] V. Sidorenko and M. Bossert, "Decoding interleaved Gabidulin codes and multisequence linearized shift-register synthesis," in *Proc. of 2010 IEEE International Symposium on Information Theory, ISIT'10*, 2010.
- [10] R. Overbeck, "Public key cryptography based on coding theory," *Ph.D. Thesis*, 2007.
- [11] E. Arkan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theor.*, vol. 55, no. 7, pp. 3051–3073, 2009.
- [12] M. Seidl and J. Huber, "Improving successive cancellation decoding of polar codes by usage of inner block codes," *Turbo Codes and Iterative Information Processing, 2010 6th International Symposium on*.
- [13] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press, 1994.